UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA
Allentown Division

Chev. Rev. Edward Thomas Kennedy,

Plaintiff.

v.

Charlie Dent,

Nina E.Olson,

John Koskinen,

Case :_____

Paulino do Rego Barros, Jr.,

Richard Smith,

Equifax Inc.

Defendants.

Complaint Jury Trial Demanded

Plaintiff is Chev. Rev. Edward Thomas Kennedy for a Complaint and Demand For Jury Trial against Defendants Charlie Dent, Nina E.Olson, John Koskinen, Paulino do Rego Barros, Jr.,Richard Smith, and Equifax Inc. alleges as follows:

1. This is an action to request personal injury damages for Identity Theft and relief from alleged tax debt and penalties caused by Identity Theft caused by data breaches thereof;

PLAINTIFF

1. Plaintiff's title is Chevallier Reverend. Plaintiff is a Papal Knight, holds a Diplomatic Passport Number: QS01003115, is ordained as Roman Catholic Priest, Eastern Rite, Apostolic Ecclesiastic Number: 1003115, Date of Ordination: November 17, 2013.

2. Plaintiff is both a Missionary Roman Catholic Priest in the Sacred Medical Order Church of HOPE or SMOCH, and a Knight in the Sacred Medical Order Knights of HOPE, where the word HOPE translates and means Hospitaller Order of Physicians & Ecclesiae.

3. Plaintiff has taken Oaths with an Investiture in 2008, and obeys that oath and says only now fully realizes the full extent of the matter.

4. Plaintiff's parish is on Nevis Island but Plaintiff's Church and principal place of my Church now and related Medical Charity is within the District at 401 Tillage Road, Breinigsville, PA 18031.

5 Plaintiff holds an MBA or Masters degree in Business Administration from The Graduate School of the University of Notre Dame, now called Mendoza, with a concentration in accounting and federal income tax. James L. Wittenbach is a Full Professor in the Department of Accountancy since 1972, link:
http://mendoza.nd.edu/research-and-faculty/directory/jim-wittenbach/
and he was one of my teachers.

6. Plaintiff is mainly a missionary Roman Catholic priest, not a BAR Member and is not an experienced litigator, and requests the Court to assist with unintentional errors made herein, such as statutes or codes citations, interpretation of local rules and federal rules of evidence and federal rules of procedure. Concerning local rules, and based on Plaintiff's status on both funds and health, Plaintiff requests this case remain within the Allentown District for Plaintiff is disabled and poor.

DEFENDANT

7. Defendant Charlie Dent is US Representative, and is at 3900 Hamilton Blvd #207, Allentown, PA 18103.

8. Defendant Nina E. Olson, is the National Taxpayer Advocate, and is at Internal Revenue Service, 1111 Constitution Avenue Northwest, Washington, DC 20224. IRS Taxpayer Advocate is a creation of US Congress, and Defendant Dent has authority over it.

9. Defendant John Koskinen is the 48th IRS Commissioner. and as Commissioner, he presides over the nation's tax system, is located at 1111 Constitution Avenue Northwest, Washington, DC 20224.

10. Defendant Paulino do Rego Barros, Jr., is Interim Chief Executive Officer, Equifax Inc.is at 1550 PEACHTREE ST NW, ATLANTA, GA 30302, Phone: 404-8858000

11, Defendant Richard Smith, is former Chief Executive Officer, Equifax Inc.and can be reached at 1550 PEACHTREE ST NW, ATLANTA, GA 30302, Phone: 404-8858000

12. Defendant Equifax Inc.,is at 1550 PEACHTREE ST NW, ATLANTA, GA 30302, Phone: 404-8858000

JURISDICTION AND VENUE

12. This court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. SS 1331 and 1338(a) and (b), in that this is an action for false designation of origin under 15 U.S.C. S 1125(a) and unfair competition. The court also has supplemental jurisdiction over the state law claims asserted herein under 28 U.S.C. S

1367(a).

13. Personal jurisdiction and venue are proper in this Judicial District. Defendants reside in this District. Defendants have transacted and purportedly are transacting business in this District, which has given rise to the claims in this lawsuit.

Plaintiff's paper tax return was mailed and filed for 2016 with zero income from 401 Tillage Road, Breinigsville, PA 18031 on April 14, 2017 and Plaintiff recently received a tax bill from IRS at the location.

BACKGROUND FACTS

14. Plaintiff asked Charlie Dent to help the Plaintiff in the last 12 to 18 months and services under the taxpayer Bill of Rights and Taxpayer Advocate website, relief was not granted for unknown reasons.

15. To file federal income taxes with "income," from the beginning, Plaintiff only used Intuit software, usually purchased at Costco at discount. In 2001 and 2002 (Plaintiff paid a large sum in federal and state incomes taxes due to profits from silicon valley startups, and used Intuit software to prepare, calculate and file tax returns. Plaintiff became sick and has not worked for wages or investments since that time but has performed medical charity for the poor.)

(* Except for calendar year 2016, Plaintiff did not use Intuit Software and filed with paper for LSAC.org proof concerning no income waiver to apply to Law Schools for Fall 2018 admissions.)

16. Plaintiff, is now a Roman Catholic priest, but in 2001, was married to Sharon Maj Gordano, at 4 Binnacle Ln, Foster City, CA 94404, and Sharon at the time was a high level Marketing Executive at Intuit, and responsible for Privacy.

17. Plaintiff says at trial, Plaintiff will ask Sharon to reluctantly testify about NO DATA ENCRYPTION and thus NO privacy of data at IRS but also all three credit reporting agencies, including Equifax. Plaintiff says Sharon resigned from Intuit in 2002 or 2003 to work for a non-for profit at at dramatically reduced salary.

18. IRS uses no data encryption, and thus is open to data theft, evidenced by Exhibit 3, 3 pages, Letter to John Koskinen, Commissioner of the Internal Revenue Service - IRS Data Breach, Letter By: US Representatives Paul Ryan and Peter Roskam Date: May 29, 2015, **Location:** Washington, DC.

19 Equifax uses no data encryption, and thus is always open to data theft.

20. Plaintiff said former CEO Richard Smith lied to Congress when he said only one guy was to blame for the data breach. Exhibit 4, one page. "Former Equifax CEO Blames One IT Guy for Massive Hack." Plaintiff says all Equifax data was stolen for there is no data encryption.

21. Plaintiff says Richard Smith made a business decision not to encrypt any data so he could sell ID Data protection services. Exhibit 5, "How Equifax is Making Millions of Dollars Off Its Own Screw Up."

22. Intuit uses data encryption, and thus always was used by Plaintiff to file when Plaintiff had income.

23. Plaintiff's ID and data was stolen, and false returns were filed in order to harm me, and Plaintiff does not know by whom.

24. Plaintiff's personal ID data was sold on the dark internet.

25. Plaintiff says the name Edward Kennedy is a magnet for haters just as the name Donald J Trump is a magnet for haters but the name Edward Kennedy was a magnet for headers longer than current US President Trump.

27. Plaintiff says former CEO Richard Smith made a prudent business decision not to encrypt customer data held in Equifax computers because the cost was not worth the benefit to Equifax shareholders and no encryption also provided Equifax a business opportunity to market and sell data Protection Services on an annual subscription basis, a good profitable, long term business strategy.

28. Plaintiff says that Defended and IRS Commissioner John Koskinen, and National taxpayer Advocate Nina E. Olson made prudent business decisions to protect their data vendor, especially Defendant Equifax, for they depend upon the credit bureaus for data.

29. Plaintiff says that it was not a prudent decision for former Equifax CEO Richard Smith and IRS Commissioner John Koskinen, and National taxpayer Advocate Nina E. Olson to lie to Congress about data security and data breaches.

30. Plaintiff says all 10 of Taxpayer Bill of Rights were not granted or violated by the IRS Taxpayer Advocate. link: https://www.irs.gov/pub/irs-pdf/p5170.pdf,
10 Taxpayer Bill of Rights are as follows:
The Right to Be Informed
The Right to Quality Service

The Right to Pay No More than the Correct Amount of Tax
The Right to Challenge the IRS's Position and Be Heard
The Right to Appeal an IRS Decision in an Independent Forum
The Right to Finality
The Right to Privacy
The Right to Confidentiality
The Right to Retain Representation
The Right to a Fair and Just Tax System.

31. Plaintiff has been sick with infections that affected my marriages and jobs and behaviors since 1985, and this allowed these matters to continue. Plaintiff now believes now only depression remains.

32. Plaintiff was not informed about the full extent of the alleged debt until 38 minute conversation with IRS employee, Mr. Gonzales, Exhibit 1, Identity Theft Report, FTC report Number 8711809, two pages, his recommendation to file and submit the Attached Exhibit 2, one page, IRS Form 14039, Identity Theft Affidavit to IRS offices in Fresno, Andover and Kansas City and this task was completed on Tuesday, October 25, 2017.

33. Plaintiff received a bill from IRS Andover, MA office at 401 Tillage Road, Breinigsville, PA 18031 on Monday, October 24, 2017, IRS document Notice of Intent to Seize (levy) your property or rights to property, demanding payment.

34. Plaintiff promptly called IRS and told IRS employee Mr. Gonzales, that Plaintiff is a priest, disabled, poor and it now a victim of Identity Theft.

35. IRS employee said their investigation would take 180 days.

36. Plaintiff told IRS employee this is too long for it affects my ability now to function as a missionary priest and also affects my ability to borrow money for law school and also apply for grants.

37. Plaintiff is registered at LSAC.org, Account #: L38059298, and plans to become a BAR Attorney and this matter prevents me from borrowing money for law school, and thus request Relief from the Court from the odious alleged debt by IRS.

FIRST COUNT

(Violation of Identity Theft and Assumption Deterrence Act

18 USC 1028, 1998.)

38. Plaintiff repeats and realleges herein the allegations of paragraphs 1-37 of this Complaint.

39. Defendant's acts caused extreme trauma to Plaintiff and have damaged Plaintiff physically and mentally and spiritually.

40. Unless restrained and enjoined, Defendant's conduct has caused, and will continue to cause Plaintiff great and irreparable harm.

41. Plaintiff does not have an adequate remedy of law.

42. Plaintiff is entitled to recover damages under Violation of Identity Theft and Assumption Deterrence Act 18 USC 1028, 1998 and related law..

SECOND COUNT

(Internal Revenue Service Restructuring and Reform Act of 1998. The Internal Revenue Service Restructuring and Reform Act of 1998, also known as Taxpayer Bill of Rights III, (Pub.L. 105–206, 112 Stat. 685, enacted July 22, 1998)

43. Plaintiff repeats and realleges herein the allegations of paragraphs 1-42 of this Complaint.

44. Defendant's acts have damaged Plaintiff.

45. Unless restrained and enjoined, Defendant's conduct has caused, and will continue to cause Plaintiff great and irreparable harm.

46. Plaintiff does not have an adequate remedy of law.

47. Plaintiff is entitled to recover damages and seeks debt forgiveness from the beginning and that my positive credit status to borrow funds for law school be restored.

THIRD COUNT

(Conspiracy to harm Plaintiff and

Canon law and Common law harm to a Priest and Knight)

48. Plaintiff repeats and realleges herein the allegation of paragraphs 1-47 of this Complaint.

49. By reason of the foregoing, Defendants have engaged in intentional infliction of emotional distress.

50. Plaintiff is entitled to recover damages and seeks debt forgiveness from the beginning and that my positive credit status to borrow funds for law school be restored.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. Order IRS to pardon and forgive all alleged debts from the beginning.

B. Awarding the Plaintiff its damages for Identity Theft and Equifax's failure to protect Plaintiff data from unknown hackers from only Equifax.

C. Awarding the Plaintiff damages for personal injury(s) as may be established upon the trial of this action;

D. Awarding the Plaintiff damages for personal injury(s) and related loss of reputation in the community;

E. Granting Plaintiff such other and further relief as to the court deems just and proper.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge,

DATED this 27th day of October, 2017.

Chev. Rev. Edward Thomas Kennedy.
Sacred Medical Order Knights of HOPE Hospitaller Order of Physicians & Ecclesiae.
Sacred Medical Order Church of HOPE Hospitaller Order of Physicians & Ecclesiae.
401 Tillage Road
Breinigsville, Pennsylvania 18031.
Phone 415-275-1244.
Email: kennedy2008@alumni.nd.edu.

EXHIBIT 1

FEDERAL TRADE COMMISSION

Identity Theft Report

FTC Report Number:
87118409

I am a victim of identity theft. This is my official statement about the crime.

Contact Information

Father Edward Thomas Kennedy
401 Tillage Road
Breinigsville, 18031

415-275-1244
kennedy2018@alumni.nd.edu

Personal Statement

I ran as a Candidate in the special statewide election for California Governor in 2003, as a Democrat, and the Attorney for the Democratic Party told me privately my ID, name Edward Kennedy, a magnet for haters, had been stolen. I only learned about the full extent of the problem today, from the IRS, Mr. Gonzales, IRS Employee # 100-30-72-427. I studied tax at Notre Dame University Graduate Business school, and at one time was Certified as a Preparer in California. I last used Intuit software in either 2001 or 2002. I ordered transcripts. Equifax does not encrypt their data, in order to sell insurance or protection. I submitted IRS Form 14039, a new Form, today. I have mostly been sick with infections since 2001 and suffer from depression. I am now a Roman Catholic Priest, Eastern Rite, and a Papal Knight, Hospitaller Order, and have relied on charity from my family. I hope to fix this fast in order to borrow funds to go to Ave Maria Law School in Florida in Sept. 2018.

Tax Fraud

Date that I discovered it
10/2017

Fraudulent Information on Credit Reports

Accounts or Charges	No, not at this time

Under penalty of perjury, I declare this information is true and correct to the best of my knowledge.

I understand that knowingly making any false statements to the government may violate federal, state, or local criminal statutes, and may result in a fine, imprisonment, or both.

Father Edward Thomas Kennedy

10/24/2017.
Date

Use this form to prove to businesses and credit bureaus that you have submitted an identity theft report to law enforcement. Some businesses might request that you also file a report with your local police.

EXHIBIT 2

Form 14039 (April 2017)	Department of the Treasury - Internal Revenue Service **Identity Theft Affidavit**	OMB Number 1545-2139

Complete this form if you need the IRS to mark an account to identify questionable activity.

Section A – Check the following boxes in this section that apply to the specific situation you are reporting *(Required for all filers)*

X 1. I am submitting this Form 14039 for myself

X 2. This Form 14039 is submitted in response to a 'Notice' or 'Letter' received from the IRS
- Please provide 'Notice' or 'Letter' number(s) on the line to the right _____
- Please check box 1 in Section B and see special mailing and faxing instructions on reverse side of this form.

3. I am submitting this Form 14039 on behalf of my 'dependent child or dependent relative'.
- Please complete Section E on reverse side of this form.
Caution: If filing this on behalf of your 'dependent child or dependent relative', filing this form will protect his or her tax account but it will not prevent the victim in Section C below from being claimed as a dependent by another person.

4. I am submitting this Form 14039 on behalf of another person *(other than my dependent child or dependent relative)*.
- Please complete Section E on reverse side of this form.

Section B – Reason For Filing This Form *(Required)*

Check only ONE of the following boxes that apply to the person listed in Section C below.

✓ 1. Someone used my information to file taxes

2. I don't know if someone used my information to file taxes, but I'm a victim of identity theft

Please provide an explanation of the identity theft issue, how you became aware of it and provide relevant dates. If needed, please attach additional information and/or pages to this form.

See Attached Identity Theft Report (2 sides)

FTC Report Number 871118409

Section C – Name and Contact Information of Identity Theft Victim *(Required)*

Victim's last name	First name	Middle initial	Taxpayer Identification Number *(Please provide 9-digit Social Security Number)*
Kennedy	Father Edward	Thomas	197445450

Current mailing address *(apartment or suite number and street, or P.O. Box)* If deceased, please provide last known address
401 Tillage Road

Current City	State	ZIP Code
Breinigsville	PA	18031

Tax Year(s) you experienced identity theft *(If not known, enter 'Unknown' in one box below)*	What is the last year you filed a return
UNKNOWN	2012 *

Address used on the last filed tax return *(if different than 'Current')*	Names used on last filed tax return *(if different than 'Current')*
4 BIANNITE LN	

City *(on last tax return filed)*	State	ZIP Code
Foster City	CA	94404

Telephone number with area code *(Optional) If deceased, please indicate 'Deceased'*

Home telephone number	Cell phone number	Best time(s) to call
415 275 1244		Anytime

Language in which you would like to be contacted X English ___ Spanish

Section D – Penalty of Perjury Statement and Signature *(Required)*

Under penalty of perjury, I declare that, to the best of my knowledge and belief, the information entered on this Form 14039 is true, correct, complete, and made in good faith. Father Edward Thomas Kennedy

Signature of taxpayer, or representative, conservator, parent or guardian	Date Signed
Father Edward Thomas Kennedy	10/25/2017.

Submit this completed form to either the mailing address or the FAX number provided on the reverse side of this form.

* AND NOW 2016

EXHIBIT 3

Letter to John Koskinen, Commissioner of the Internal Revenue Service - IRS Data Breach

votesmart.org/public-statement/978201/letter-to-john-koskinen-commissioner-of-the-internal-revenue-service-irs-data-breach

May 28, 2015

The Honorable John Koskinen
Commissioner
Internal Revenue Service
1111 Constitution Avenue, NW
Washington, DC 20224

Dear Commissioner Koskinen:

Taxpayer confidence in the Internal Revenue Service's (IRS) ability to safeguard personal information is critical to our nation's system of voluntary tax compliance. The IRS's announcement that cyber attackers took advantage of IRS system vulnerabilities to access 104,000 taxpayers' confidential information is a profound mission failure. We are writing to inquire about the full extent of the breach, including whether these crimes were facilitated by known system weaknesses and what steps the IRS is taking to prevent any further breaches.

In recent months, both the Treasury Inspector General for Tax Administration (TIGTA) and the Government Accountability Office (GAO) identified significant deficiencies in the IRS's information security systems. In particular, they found that the IRS's systems did not have appropriate identity and access management (IA&M), leaving them vulnerable to cyber attacks, including unauthorized access to personally identifiable information. Further, they found that the systems had weak configuration management, which would prevent administrators from monitoring and controlling changes to IRS IT systems.

On May 26, 2015, the IRS announced that its online Get Transcript service, established in January 2014, had been exploited, providing improper access to 104,000 taxpayers' confidential information. The IRS reported that before it detected the unauthorized access, it issued 15,000 fraudulent refunds, totaling about $50 million. Until now, the IRS has been promoting its Get Transcript application nationally as providing safe and streamlined customer service.

But in its review of the IRS's information systems, TIGTA found that for FY 2014, the IRS was fully compliant with fewer than half of the performance metrics established by the Federal Information Security Management Act of 2002 (FISMA). FISMA establishes a clear framework for how government agencies must protect information and information systems, support the safe and secure adoption of new technology, and create a sophisticated information security workforce. It is essential that the IRS maintains FISMA standards to protect taxpayer information, but TIGTA reported that only five of eleven security areas met all FISMA requirements. Two key areas--configuration management and identity and access management--failed to meet the majority of standards needed for compliance.

Strong configuration management is important because it creates stability and efficiency within a system and allows administrators to identify and address problems quickly. Appropriate IA&M is key to preventing cyber attacks because it ensures that only people with proper identification and authentication may access systems. Weak IA&M can leave systems vulnerable to cyber attacks, including social engineering, and can make it difficult or impossible to identify whether unintended users are accessing information within the system.

Similarly, in March 2015, GAO released a report highlighting numerous weaknesses in the IRS's systems. GAO found that the IRS did not have strong password protection controls; IRS employees had excessive access privileges that allowed them to see information not necessary for their jobs; and physical access controls were inconsistent.

Additionally, the IRS's servers used weak encryption--or no encryption at all--to authenticate users, potentially allowing unauthorized users to view data and then use that information to gain access to the systems.

Both GAO and TIGTA have reported that these weaknesses leave taxpayer information vulnerable to attack. TIGTA concluded that:

[U]ntil the IRS takes steps to improve its security program deficiencies and fully implements all 11 security program areas required by the FISMA, taxpayer data will remain vulnerable to inappropriate use, modification, or disclosure, possibly without being detected.

GAO's findings matched TIGTA's conclusions:

Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intentions who can intrude and use their access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks . . . threats include the ever-growing number of cyber-based attacks that can come from a variety of sources--individuals, groups, and countries who wish to do harm.

These security safeguards are extremely important, especially as the government relies more and more on information technology.

The IRS has a responsibility to protect taxpayer information from unauthorized access and attacks. Clearly, the agency needs to do more. In order for the House Ways and Means Committee to better understand the breach that resulted in 104,000 taxpayers' information being compromised and the steps the IRS is taking to prevent future unauthorized disclosures, please respond to the following questions by June 11, 2015:

Describe the IRS's Get Transcript application generally, as well as any other systems affected by the cyber attack.

When and how did the IRS discover the cyber attack? Did any IRS detection involve algorithmic analysis, including analysis of account access patterns, transcript request trends, number or frequency of password reset attempts, etc.? If so, please describe the indicators detected and how IRS systems are designed to screen for them.

Did the IRS discover the problems itself, or did another organization or person call the problems to the IRS's attention? If so, who, when, and how did they inform the IRS?

We understand that 104,000 taxpayers' information was compromised. Were the 104,000 taxpayers part of a discrete group, or were they a random selection from the pool of taxpayers?

What data were accessed by the attackers?

Is the IRS assured that no other taxpayers' information, beyond those identified above, was compromised? If so, how?

Is the IRS reviewing its other applications, such as Where's My Refund, IRS Direct Pay, and IRS Online Payment Agreement, to determine if they are vulnerable or have been subject to an attack?

What steps is the IRS taking to notify potential victims of the attack?

What determinations has the IRS made about the cause of the attack? Who carried out the attack? What vulnerabilities allowed the attack to occur?

The IRS has reported that the criminals who carried out the attacks were able to answer "out of wallet" questions in order to access the system. What types of "out of wallet" questions does the IRS use to verify taxpayers? What steps will the IRS take to strengthen its authentication of users?

What steps will the IRS take to protect the 104,000 accounts from further unauthorized access or related crimes, such as identity theft related tax fraud?

Is the IRS coordinating with other agencies to investigate the attack and/or prevent taxpayer information from being used to perpetuate fraud in other federal programs? If yes, please describe all coordination efforts.
Please provide all information on any improvements the IRS has made to its information security to address TIGTA's and the GAO's recommendations.

Please provide a summary of any outstanding information security weaknesses, including any current agency efforts to resolve them and/or future plans to resolve them.

Additionally, please provide a briefing for Ways and Means Oversight Subcommittee staff on the cyber attack, no later than June 12, 2015.

Thank you for your attention to this extremely important matter. If you have any questions about this request, please do not hesitate to contact Oversight Subcommittee staff at (202) 225-5522.

Sincerely,

PAUL D. RYAN PETER J. ROSKAM
Chairman Chairman
Committee on Ways and Means Subcommittee on Oversight

Source: http://waysandmeans.house.gov/ryan-roskam-demand-answers-on-irs-data-breach-2/

EXHIBIT 4

Former Equifax CEO Blames One IT Guy for Massive Hack

nbcnews.com/business/consumer/former-equifax-ceo-blames-one-it-guy-massive-hack-n807956

by Ben Popken

Disgraced former Equifax CEO Richard Smith spent the week giving an apology tour on Capitol Hill, explaining to lawmakers exactly how his credit bureau failed to prevent a historic data breach that allowed 145.5 million Americans to have their personal financial history made public.

While Smith said he was personally "ultimately responsible for what happened" he also blamed a single unnamed person in the IT department for not updating, or "patching" one Equifax's "portals" after the credit reporting giant was alerted to the security gap in March.

"An individual did not ensure communication got to the right person to manually patch the application," Smith testified before the Senate Banking Committee on Wednesday.

He also said the company's scanning software, which looks for unpatched systems, didn't find the hole — all of this despite "investments approaching a quarter of a billion dollars in security," Smith acknowledged.

'Monopoly Man' Photobombs Former Equifax CEO's Congressional Hearing 0:57

Related: The One Move to Make After Equifax Breach

Legislators took turns blasting the ex-CEO during his three days of back-to-back testimony, lambasting him for the historic breach and for Equifax's "haphazard" and "sloppy" response to it.

"The criminals got everything they need to steal your identity," said Texas Congressman Jeb Hensarling, Chairman of the House Financial Services Committee, in his opening remarks Thursday. "This may be the most harmful attack on a company's personal information the world has ever seen." He called for action by Congress, the Federal Trade Commission, the Consumer Financial Protection Bureau, and other regulators to hold the company to account and prevent future breaches.

"The status quo is clearly failing consumers," said Hensarling.

Members of the Senate Banking Committee also took issue with the fact that Equifax was just awarded a $7 million government contract to help prevent IRS fraud.

"That looks like we're giving Lindsay Lohan the key to the minibar," said Senator John Kennedy of Louisiana.

Lawmakers took Smith to task on several other fronts: the failure to notify customers for a month that their data had been stolen, executives selling company stocks the day before Equifax notified the FBI of the breach, and a "glitchy" remediation website and customer support lines.

Related: FTC Launches Equifax Probe, Websites and Phones Jammed With Angry Consumers

"Because of this breach, consumers will spend the rest of their lives worrying about credit history," said Massachusetts Senator Elizabeth Warren. "But Equifax will be just fine, it could actually come out ahead!"

She and other lawmakers pointed out how Equifax could stand to make more money from consumers rushing to purchase identity theft protection products like Lifelock. It happens that Lifelock is a client of Equifax and pays Equifax for the data it uses to power its services — which means consumers are paying a customer of Equifax's who pays Equifax to protect themselves from Equifax's failings.

How Equifax Is 'Making Millions of Dollars Off Its Own Screwup'

fortune.com/2017/10/04/equifax-breach-elizabeth-warren/

Just three weeks before Equifax disclosed a colossal data breach that compromised the data of more than 145 million people, its then-CEO Richard Smith gave a speech in which he declared that "fraud is a huge opportunity for us."

Now, Senator Elizabeth Warren (D-Mass.) is making Equifax (EFX, -0.57%) and its former CEO rue those words. A day after berating Wells Fargo CEO Tim Sloan over the bank's own scandal with phony accounts, Senator Warren took aim Wednesday at Smith, who retired as CEO of the credit reporting agency last week in the wake of the Equifax breach.

Smith faced Congress for the second day in a row to offer his testimony on the massive hack, part of a three-day schedule of hearings on Capitol Hill.

Quoting Smith's earlier comments, delivered at the University of Georgia business school in August, Warren, an outspoken consumer watchdog, accused him of not only injuring Americans affected by the Equifax breach, but of profiting off their plight.

After Smith conceded that the Equifax hack had increased the likelihood of fraud, the Senator used his own words against him: "So the breach of your system has actually created more business opportunities for you," Warren said Wednesday at a hearing of the Senate banking committee.

For one, Warren pointed out, 7.5 million people have signed up for the free year of credit monitoring that Equifax offered following the breach, but after that, they will have to pay Equifax $17 a month to continue the service. If just one million of those people opt to do so, it amounts to an additional $200 million in revenue for Equifax, Warren said. If they all do, Equifax stands to make more than $1.5 billion extra.

What's more, LifeLock, an identity theft protection company, has said that enrollments for its service have increased 10-fold since the Equifax breach, with more than 100,000 signing up within just the first week after the hack was disclosed. But LifeLock, whose protection plans cost up to $29.99 a month, buys its credit monitoring service from Equifax—meaning that Equifax is still getting a cut of those sales, Warren said.

"You've got three different ways that Equifax is making money, millions of dollars, off its own screwup," the Senator said at the hearing.

The third way Equifax may benefit, Warren explained, is through the products it sells to government agencies to help them with identity verification, something that could be all the more important if the breach leads to greater identity theft, as expected. For example, it was also revealed Wednesday that the IRS just signed a new $7.25 million contract with Equifax in September, after the breach was announced.

In short, the Senator argued, Equifax has far more to gain from its data breach than it does to lose, with the average victim of a data breach receiving a payout of just $2 in restitution, she said.

"Consumers will spend the rest of their lives worrying about identity theft," Warren continued. "But Equifax will be just fine—heck, it could actually come out ahead."

Equifax's former CEO Smith will continue his testimony on Thursday when he appears before the House Financial Services Committee at 9:15 a.m. E.T.